Datenschutzrecht

Februar 2017

Dynamische IP-Adressen als personenbezogene Daten

Der Europäische Gerichtshof (EuGH) hat im Oktober 2016 entschieden, dass dynamische IP-Adressen für Webseitenbetreiber als personenbezogene Daten zu qualifizieren sein können, wenn der Webseitenbetreiber über rechtliche Mittel verfügt, den betreffenden Nutzer mithilfe des Internetzugangs bestimmen zu lassen (EuGH, Urt. v. 19.10.2016 – C-582/14). Hintergrund der Entscheidung war die Klage eines deutschen Internetnutzers, der die längerfristige Speicherung der seinem Internetanschluss zugewiesenen dynamischen IP-Adresse durch einen Webseitenbetreiber beanstandet hat. Diese Speicherung erfolgte nach Auskunft des Webseitenbetreibers, um sich gegen Cyberattacken verteidigen zu können und eine Strafverfolgung zu ermöglichen. Dieses Vorgehen hat der EuGH als zulässig bewertet.

Damit hat der EuGH gleich zwei grundsätzliche Entscheidungen getroffen: Zum einen steht nun fest, dass auch dynamische IP-Adressen als personenbezogene Daten anzusehen sein können. Im Gegensatz zu statischen IP-Adressen ermöglichen dynamische IP-Adressen es nicht, den Internetnutzer bereits aufgrund der dauerhaften Verbindung einer IP-Adresse zu einem bestimmten Netzanschluss zu identifizieren. Vielmehr kann dies erst durch die Einbindung des Internet Access Providers geschehen, wenn dieser unter Verwendung von Verkehrsdaten (wie z. B. Datum und Uhrzeit der konkreten Internetverbindung) den der IP-Adresse zugewiesenen Anschlussinhaber ermittelt. Der EuGH hat jetzt klargestellt, dass es bereits ausreicht, dass der Webseitenbetreiber über die rechtlichen Mittel verfügt, um an die zur Identifizierung des Nutzers erforderlichen Zusatzinformationen zu gelangen. Ist dies der Fall, handelt es sich auch bei der dynamischen IP-Adresse um ein personenbezogenes Datum.

Zum anderen hat der EuGH die bisher enge Auslegung des § 15 Telemediengesetz (TMG) für unvereinbar mit der Datenschutzrichtlinie (95/46/EG) erklärt. Nach dieser deutschen Vorschrift dürfen Diensteanbieter (wie z. B. Betreiber von Webseiten) personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit das erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Da diese Regelung bei enger Auslegung keinen Raum für die von Art. 7 lit. f der Datenschutzrichtlinie geforderte Interessenabwägung lässt, verstößt eine solche Auslegung nach Auffassung des EuGH gegen das zugrundeliegende EU-Recht. Vielmehr müsse im Wege einer richtlinienkonformen Auslegung das berechtigte Interesse des Diensteanbieters mit den Grundrechten der betroffenen Personen abgewogen werden, was durchaus zu einem überwiegenden Interesse des Webseitenbetreibers an der Aufrechterhaltung der Funktionsfähigkeit seiner Webseite führen könne.

Praxishinweis
Webseitenbetreiber und sonstige Online-Diensteanbieter sollten stets davon ausgehen, dass es sich bei IP-Adressen um personenbezogene Daten handelt. Dies galt zuvor schon für statische IP-Adressen und ist nun auch auf dynamische IP-Adressen übertragbar. Da der Webseitenbetreiber regelmäßig auch gar nicht weiß, ob der Zugriff des Nutzers auf die Webseite mittels einer statischen oder einer dynamischen IP-Adresse erfolgt, sollten die datenschutzrechtlichen Vorgaben in jedem Fall beachtet werden. Vor diesem Hintergrund hat der EuGH zwar einen juristisch bedeutsamen Streit entschieden. Die praktischen Konsequenzen für Webseitenbetreiber sind insoweit jedoch überschaubar.

Weitaus größere praktische Relevanz hat das Urteil jedoch für die Definition von personenbezogenen Daten und damit für die grundsätzliche Anwendbarkeit der Datenschutzgesetze. Wenn es sich hierbei um persönliche und sachliche Verhältnisse einer *bestimmten* oder *bestimmbaren* natürlichen Person handelt (vgl. § 3 Abs. 1 BDSG), dann ist der Kreis der Bestimmbarkeit zukünftig deutlich weiter zu ziehen als bisher. Denn nach dem EuGH kommt es nicht darauf an, dass der Webseitenbetreiber selbst über die Zusatzinformationen verfügt, um einen Nutzer zu identifizieren, dem in einem bestimmten Zeitpunkt eine dynamische IP-Adresse zugewiesen ist. Vielmehr soll bereits ausreichen, dass er die rechtlichen Mittel hat, um sich solche Zusatzinformationen zu verschaffen. Da das deutsche Recht unter verschiedenen Voraussetzungen Auskunftsansprüche gegen Internetserviceprovider zur Verfügung stellt, mit denen die Identität von Internetnutzern z. B. im Falle von online begangenen Urheberrechtsverletzungen ermittelt werden kann, stehen die rechtlichen Mittel zur Verfügung, um an die notwendigen Zusatzinformationen zur Identifizierung des hinter einer dynamischen IP-Adresse stehenden Nutzers zu gelangen. Dies kann sich zukünftig möglicherweise noch auf ganz andere Bereiche auswirken, in denen es auch nur potentiell möglich ist, Nutzer anhand von Zusatzinformationen zu identifizieren, beispielsweise über sog. mobile device identifiers. Hier dürfte sich bald nicht nur die Frage stellen, wer solche technischen Hilfsmittel unter welchen Voraussetzungen einsetzen darf, sondern auch, wer unter welchen Voraussetzungen einen Anspruch auf die über diese Hilfsmittel erhaltenen Informationen hat. Dies könnte dazu führen, dass zukünftig viel häufiger der Personenbezug von Daten zu bejahen sein wird, als es bisher der Fall war.

Die Feststellung des EuGH, dass die bisherige enge Auslegung von § 15 TMG nicht mit EU-Recht vereinbar ist, wird nicht unbedingt zur Rechtssicherheit in diesem Bereich beitragen. Zwar ermöglicht eine richtlinienkonforme und damit weitere Auslegung es dem Webseitenbetreiber, die bei der Nutzung von Online-Diensten anfallenden Daten ggf. über einen längeren Zeitraum und zu anderen als den in der Norm genannten Zwecken zu speichern. Dies wird aber unweigerlich Folgefragen über die zulässige Speicherdauer unter Berücksichtigung des jeweiligen, dann nicht gesetzlich normierten, Zwecks nach sich ziehen. Der vom EuGH geforderten Interessenabwägung wird daher zukünftig großes Gewicht beizumessen sein. Dennoch werden wohl die nationalen Gerichte die neuen Grenzen des § 15 TMG ausloten müssen.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht

Datenübertragung nach dem EU-U.S. Privacy Shield

Seit dem 1. August 2016 können sich Unternehmen zum sog. Privacy Shield, dem Nachfolger des „Safe Harbor"-Abkommens, anmelden, sich also durch das US-Handelsministerium zertifizieren lassen. Mit diesem neuen Abkommen soll die Übertragung personenbezogener Daten in die USA sowohl für europäische als auch für US-Unternehmen wieder vereinfacht werden. Hintergrund ist, dass der

EuGH mit Entscheidung vom 6. Oktober 2015 das „Safe Harbor"-Abkommen für ungültig erklärt hatte, so dass die in der Praxis wichtigste Rechtsgrundlage für den transatlantischen Datentransfer entfallen war (siehe hierzu unsere Newsletter „EuGH kippt Safe-Harbor" von Oktober 2015 und „Annahme des EU-U.S.-Privacy-Shield durch die Europäische Kommission" von Juli 2016).

Praxishinweis
Nach dem Ende des „Safe Harbor"-Abkommens war Unternehmen in der Regel zu raten, ihre Datenübertragung in die USA auf die Verwendung der „EU-Standardvertragsklauseln" oder auf unternehmensweite „Binding Corporate Rules" zu stützen. Sofern Unternehmen ihren transatlantischen Datenverkehr mittlerweile auf diese alternativen Rechtsgrundlagen gestellt haben, ist eine nochmalige Umstellung auf den Datentransfer unter dem „Privacy Shield" vorerst nicht notwendig. Zurzeit erscheint dies auch nicht sinnvoll: Schon vor Inkrafttreten des „Privacy Shield" wurde das Abkommen heftig kritisiert und es bleibt abzuwarten, ob es einer gerichtlichen Überprüfung durch den EuGH standhalten wird.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht

Wettbewerbswidrige Einbindung des „Facebook Like Buttons" auf der eigenen Webseite

Das Landgericht Düsseldorf hielt die Einbindung des sog. Like Buttons des sozialen Netzwerks Facebook auf einer Webseite für rechts- und wettbewerbswidrig und damit für abmahnfähig (Urt. v. 09.03.2016 – 12 O 151/15). Die Einbindung des „Like Buttons" führe dazu, dass unmittelbar bei Aufruf der Webseite die IP-Adresse des Nutzers an Facebook übermittelt werde, so dass schon insoweit eine Übertragung personenbezogener Daten stattfinde, ohne dass hierfür eine Rechtsgrundlage vorhanden sei. Darüber hinaus erhalte Facebook bei dieser Datenübermittlung auch konkrete Informationen über die besuchte Webseite (sog. Browserstring), die Facebook dem entsprechenden Nutzer zuordnen, dadurch personalisieren und insbesondere zu Werbezwecken nutzen könne, und dies unter Umständen auch dann, wenn der Nutzer selbst gar nicht Facebook-Mitglied oder zumindest im Zeitpunkt der Datenübertragung nicht parallel bei Facebook eingeloggt sei. Aufgrund dieser weitreichenden Funktionalitäten sei die Einbindung des „Like Buttons" ohne ausreichende Informationen der Nutzer über Zweck und Funktionsweise dieses Buttons und ohne eine entsprechende, frei widerrufliche Einwilligung der Nutzer zu dem Zugriff auf die IP-Adresse und den Browserstring, die jeweils vor dem Datenzugriff erfolgen müssten, unlauter.

Praxishinweis
Zur Vermeidung von wettbewerbsrechtlichen Abmahnungen oder Beanstandungen durch die Datenschutzaufsichtsbehörden ist Webseitenbetreibern zu raten, durch technische Vorkehrungen sicherzustellen, dass erst nach einem aktiven Klick des Nutzers auf den „Like Button" Daten an Facebook übermittelt werden. Dies gilt entsprechend auch für die Einbindung von sonstigen sog. Social Plugins anderer Anbieter. Eine praktische Lösung für den rechtskonformen Einsatz derartiger Plugins stellt der Heise Verlag mit dem System „Shariff" zur Verfügung, da hier eine Übermittlung von Daten an das jeweilige soziale Netzwerk verhindert wird, bevor der Nutzer durch einen Klick den jeweiligen Button selbst aktiviert und dadurch in die Datenübertragung aktiv einwilligt, sog. Zwei-Klick-Lösung. Unter folgendem Link steht „Shariff" als Open Source Software zum Download und zur Installation bereit: https://github.com/heiseonline/shariff. Zu beachten ist jedoch, dass auch bei Verwendung dieser Lösung die Datenverarbeitungsprozesse in der Datenschutzerklärung der betreffenden Webseite abgebildet sein müssen. So muss der Besucher der Webseite insbesondere über die durch den Klick auf die Social Plugins ausgelösten Datenübertragungen in verständlicher Weise informiert werden.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht

Rechtskonformer Einsatz von Cookies

Das Oberlandesgericht Frankfurt am Main hat entschieden, dass die Einwilligung des Nutzers einer Webseite in die Verwendung von Cookies auch durch eine vorformulierte Erklärung mit der Möglichkeit des Widerspruchs durch Entfernen eines voreingestellten Häkchens, also durch ein sog. Opt-out eingeholt werden kann (Urt. v. 17.12.2015 – 6 U 30/15). Darüber hinaus müssten die erforderlichen Informationen über die gesetzten Cookies nicht notwendigerweise unmittelbar in dieser Erklärung enthalten sein, sondern könnten auch in einem verlinkten Text wiedergegeben werden.

Praxishinweis
Nach deutschem Recht ist es ausreichend, den Nutzer in der Datenschutzerklärung (oder in speziellen Cookie-Hinweisen) über die Verwendung von Cookies zu unterrichten und ihn auf sein diesbezügliches Widerspruchsrecht hinzuweisen. Die europäische sog. Cookie-Richtlinie (ePrivacy-Richtlinie 2009/136/EG), welche in Deutschland bisher nicht umgesetzt wurde, fordert für den Einsatz von nicht zwingend notwendigen Cookies eine ausdrückliche Einwilligung des Betroffenen. Teile der Rechtsprechung nehmen daher eine richtlinienkonforme Auslegung der deutschen Vorschriften vor, und das Oberlandesgericht Frankfurt hat insoweit nun klargestellt, dass eine ausdrückliche Erklärung auch durch ein aktives Opt-out des Nutzers erklärt werden kann.

Die sicherste Vorgehensweise besteht für Webseitenbetreiber nach wie vor darin, sich die Einwilligung des Betroffenen beim ersten Aufruf der Webseite durch einen notwendigen „Klick" des Nutzers auf eine entsprechende Bannereinblendung, die mit entsprechenden Informationen über die eingesetzten Cookies versehen oder zumindest mit diesen verlinkt ist, einzuholen. Nach der Rechtsprechung des OLG Frankfurt reicht es allerdings auch aus, den Nutzer über den Einsatz von Cookies und sein Widerspruchsrecht beim ersten Aufruf zu informieren und ihm die Möglichkeit zum Opt-out einzuräumen. Diese Lösung scheint sich in der Praxis derzeit immer weiter durchzusetzen, könnte jedoch in Zukunft durch die geplante sog. ePrivacy-Verordnung der EU, die momentan im Entwurf vorliegt, wieder in Frage gestellt werden.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht

Heimliche Videoüberwachung am Arbeitsplatz: Kein Beweisverwertungsverbot bei Zufallsfunden durch verdeckte Überwachungsmaßnahmen

Das Bundesarbeitsgericht (BAG) hat in einem Urteil vom 22. September 2016 (2 AZR 848/15) wichtige Klarstellungen für

die datenschutzrechtliche Bewertung von internen Untersuchungen vorgenommen. Zusammengefasst:

- Eine verdeckte Videoüberwachung zur Aufdeckung von Straftaten von Beschäftigten darf nicht nur dann erfolgen, wenn sichergestellt ist, dass von ihr ausschließlich Arbeitnehmer betroffen sind, hinsichtlich derer es bereits einen konkretisierten Verdacht gibt. Es ist nicht erforderlich, die Maßnahme so zu beschränken, dass von ihr ausschließlich Personen erfasst werden, bezüglich derer bereits ein konkretisierter Verdacht besteht.

- Zufallsfunde aus einer gerechtfertigten verdeckten Videoüberwachung können verwertet werden.

- Die Erlaubnisnorm des § 32 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten stellt auch für die Verarbeitung und Nutzung von personenbezogenen Daten eines Beschäftigten, die der Arbeitgeber durch eine Videoüberwachung öffentlich zugänglicher Räume erlangt hat, eine eigenständige, von den Voraussetzungen der allgemeinen Vorschriften über die Videoüberwachung (§ 6b BDSG) unabhängige Erlaubnisnorm dar. Ist die Videoüberwachung über § 32 BDSG gerechtfertigt, kommt es auf die Voraussetzungen des § 6b BDSG hinsichtlich der Verwertung der Erkenntnisse gegenüber Beschäftigten nicht mehr an.

In dem entschiedenen Fall war die Klägerin bei der Beklagten, einem Unternehmen des Lebensmitteleinzelhandels, als Kassiererin tätig. Die Beklagte stellte für die Filiale der Klägerin einen Inventurverlust im Bereich Tabak/Zigaretten fest und führte im Einvernehmen mit dem Betriebsrat eine verdeckte Videoüberwachung im Kassenbereich zum Zwecke der Aufklärung von Straftaten durch, um den Diebstahl bei Zigaretten aufzudecken. Diese Videoüberwachung zielte nicht primär auf die Klägerin ab. Einer Videosequenz der verdeckten Überwachung des Kassenbereichs war zu entnehmen, dass die Klägerin unberechtigt Geld aus der Kasse genommen hatte. Daraufhin kündigte die Beklagte der Klägerin außerordentlich. Die Klägerin klagte gegen die Kündigung und berief sich auf ein Beweisverwertungsverbot wegen Verletzung ihres allgemeinen Persönlichkeitsrechts aufgrund der Verwertung datenschutzrechtswidrig erlangter Beweismittel.

Das BAG bestätigt zunächst seine ständige Rechtsprechung, dass Verstöße gegen geltendes Datenschutzrecht im Ergebnis zu einem Beweisverwertungsverbot wegen eines nicht gerechtfertigten Eingriffs in das allgemeine Persönlichkeitsrecht führen können. In diesem konkreten Fall verneint das BAG allerdings schon den Verstoß gegen das Datenschutzrecht: Die verdeckte Videoüberwachung zur Aufdeckung von Straftaten ist nach § 32 Abs. 1 Satz 1 BDSG zulässig, wenn keine milderen Mittel zur Aufklärung des fraglichen Verdachts zur Verfügung stehen. Im konkreten Fall hatte die Beklagte jedoch alle milderen Mittel bereits ausgeschöpft.

Das BAG legt für die Prüfung der Zulässigkeit einer Untersuchungsmaßnahme zur Aufdeckung von Straftaten einen objektiven Maßstab an, der auf das Vorliegen eines dokumentierten Verdachts einer Straftat – unabhängig von konkreten Verdächtigen – abstellt. Eine verdeckte Videoüberwachung zur Aufdeckung von Straftaten von Beschäftigten dürfe nicht nur dann erfolgen, wenn sichergestellt sei, dass von ihr ausschließlich Arbeitnehmer betroffen seien, hinsichtlich derer es bereits einen konkretisierten Verdacht gibt. Etwas anderes folge auch nicht aus dem Wortlaut des § 32 Abs. 1 Satz 2 BDSG. Soweit der Wortlaut der Bestimmungen ein anderes Verständnis nahelegen könne, sei er „verunglückt". Nach dem von dem BAG angelegten objektivierten Maßstab müsse zwar der Kreis der Verdächtigten möglichst eingegrenzt sein, es sei aber nicht zwingend notwendig, dass eine Überwachungsmaßnahme in der Weise beschränkt werden könne, dass von ihr ausschließlich Personen erfasst werden, bezüglich derer bereits ein konkretisierter Verdacht bestehe. Es stehe der Rechtmäßigkeit der Videoüberwachungsmaßnahme damit nicht entgegen, dass diese Maßnahme in Bezug auf die Klägerin anlasslos gewesen sei. Gebe es kein milderes Mittel zur Aufklärung des bestehenden Diebstahlverdachts gegen andere Mitarbeiterinnen als die konkret durchgeführte Überwachung, sei der Eingriff – auch – in das allgemeine Persönlichkeitsrecht der Klägerin gerechtfertigt. Eine Dokumentation des Verdachts erlaube § 32 Abs. 1 Satz 2 BDSG ebenfalls lediglich insoweit, als eine Maßnahme „zur" Aufdeckung von Straftaten erfolge.

Etwas anderes ergibt sich nach dem BAG auch nicht aus der von der Klägerin behaupteten Kollision mit den Anforderungen an Videoüberwachungsmaßnahmen aus § 6b BDSG. Das BAG stellt klar, dass die Vorschrift des § 32 Abs. 1 Satz 2 BDSG zumindest eine Konkretisierung des § 6b Abs. 1 Nr. 3 BDSG darstelle, wonach eine Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig ist. Außerdem stelle die Regelung des § 32 Abs. 1 Satz 2 BDSG auch für die Verarbeitung und Nutzung von personenbezogenen Daten eines Beschäftigten, die der Arbeitgeber durch eine Videoüberwachung öffentlich zugänglicher Räume erlangt hat, eine eigenständige, von den Voraussetzungen nach § 6b BDSG unabhängige Erlaubnisnorm dar.

Praxishinweis
Die Klarstellungen durch das BAG sind erfreulich und beziehen sich nicht nur auf Maßnahmen der Videoüberwachung. Die Grundsätze lassen sich ganz allgemein auf Untersuchungsmaßnahmen zur Aufdeckung von Straftaten in Unternehmen heranziehen. Sie geben den Verantwortlichen bei internen Untersuchungen im Hinblick auf Zufallsfunde deutlich mehr Rechtssicherheit. Mit dieser Entscheidung ist klargestellt, dass Zufallsfunde rechtmäßig durchgeführter Untersuchungsmaßnahmen verwertbar bleiben. Außerdem ist klargestellt, dass für Untersuchungsmaßnahmen nach § 32 Abs. 1 Satz 2 BDSG lediglich ein objektivierbarer Verdacht von Straftaten vorliegen muss, der die Untersuchungsmaßnahmen nicht generell nur auf einzelne Verdächtige konkretisiert. Die Erlaubnisnorm des § 32 Abs. 1 S. 2 BDSG setzt bei der Aufklärung der Tat und nicht bei den Verdächtigen an.

Für die Untersuchungspraxis ebenfalls erfreulich ist die Klarstellung, dass § 32 Abs. 1 Satz 2 BDSG im Verhältnis zu den Beschäftigten eines Unternehmens als eigenständige Rechtfertigungsgrundlage für Untersuchungsmaßnahmen dient und vermeintlich kollidierende Anforderungen aus anderen Vorschriften des BDSG (hier § 6b BDSG) für die Rechtfertigung und Rechtmäßigkeit der Maßnahme unbeachtlich bleiben. § 32 Abs. 1 Satz 2 BDSG dient insoweit als autonome Rechtsgrundlage für interne Untersuchungen zur Aufdeckung von Straftaten.

Dr. Axel von Walter
Rechtsanwalt, Fachanwalt für Urheber- und Medienrecht,
Fachanwalt für Informationstechnologierecht

Zulässige Auswertung des Browserverlaufs von Arbeitnehmern

Das Landesarbeitsgericht Berlin-Brandenburg hat entschieden, dass

die Auswertung des Browserverlaufs eines dienstlichen Internetanschlusses zum Nachweis einer exzessiven Internetnutzung von Arbeitnehmern zu privaten Zwecken nicht einem Beweisverwertungsverbot unterliegt (Urt. v. 14.01.2016 – 5 Sa 657/15). Die Speicherung und Auswertung der Verlaufsdaten sei nach dem Bundesdatenschutzgesetz zur Missbrauchskontrolle auch ohne Einwilligung des Arbeitnehmers möglich. Ein Beweisverwertungsverbot bestehe zumindest dann nicht, wenn dem Arbeitgeber der Nachweis auf andere Weise unmöglich ist.

Praxishinweis
Das Erheben, Speichern und Auswerten von Arbeitnehmerdaten ist nur unter strengen Voraussetzungen zulässig und kann für den Arbeitgeber empfindliche Bußgelder nach sich ziehen. Sofern die Datenverarbeitung nicht für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung erforderlich ist, was bei einer Datenauswertung zum Zwecke der Leistungskontrolle regelmäßig nicht der Fall ist, ist stets eine Einwilligung des Arbeitnehmers erforderlich. Allerdings wird gerade bei Arbeitnehmern die Wirksamkeit der Einwilligung in die Datenverarbeitung, sofern sie überhaupt erteilt wird, von Teilen der juristischen Literatur kritisch betrachtet, da die Freiwilligkeit der Einwilligung aufgrund der Weisungsgebundenheit des Arbeitnehmers gegenüber dem Arbeitgeber bezweifelt wird. Vor diesem Hintergrund ist die Entscheidung des Landesarbeitsgerichts Berlin-Brandenburg ein Beleg dafür, dass dem Arbeitgeber dennoch Mittel und Wege zur Verfügung stehen, wenn der Arbeitnehmer das ihm entgegengebrachte Vertrauen in eine angemessene private Nutzung des dienstlichen Internetanschlusses missbraucht.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht

Autoren

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt

Dr. Axel von Walter
Rechtsanwalt, Fachanwalt für Urheber- und Medienrecht, Fachanwalt für Informationstechnologierecht
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
München

Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie diesen Newsletter nicht mehr erhalten möchten, können Sie jederzeit per E-Mail (bitte E-Mail mit Betreff „Abbestellen" an **Melanie.Jost@bblaw.com**) oder sonst gegenüber BEITEN BURKHARDT widersprechen.

Impressum

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33, D-80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811

Weitere Informationen (Impressumsangaben) unter:
www.beitenburkhardt.com/impressum

Redaktion (verantwortlich)

Dr. Andreas Lober
Dr. Axel von Walter

Ihre Ansprechpartner

Berlin • Kurfürstenstraße 72-74 • 10787 Berlin
Tel.: +49 30 26471-0 • Fax: +49 30 26471-123
Dr. Matthias Schote • Matthias.Schote@bblaw.com

Düsseldorf • Cecilienallee 7 • 40474 Düsseldorf
Tel.: +49 211 518989-0 • Fax: +49 211 518989-29
Mathias Zimmer-Goertz • Mathias.Zimmer-Goertz@bblaw.com

Frankfurt am Main • Mainzer Landstraße 36
60325 Frankfurt am Main
Tel.: +49 69 756095-0 • Fax: +49 69 756095-512
Dr. Andreas Lober • Andreas.Lober@bblaw.com

München • Ganghoferstraße 33 • 80339 München
Tel.: +49 89 35065-0 • Fax: +49 89 35065-123
Dr. Axel von Walter • Axel.Walter@bblaw.com

Weitere interessante Themen und Informationen zum Datenschutzrecht finden Sie in unserem Onlinebereich.